COLORADO
Governor's Office of Information Technology
Serving people serving Colorado

REPORT

As Required By: SB 19-251 Section 3 CRS 24.37.5-804

Submitted on December 2, 2019, first business day after December 1st

This report is submitted pursuant to SB 19-251 Section 3 CRS 24.37.5-804, which charges the Office of Information Technology (OIT) with *"convening a working group of state agencies to determine the cost, feasibility, and appropriateness of transferring ownership of information technology infrastructure and submit a report to the JBC by December 1, 2019, regarding necessary statutory and rule changes and funding if the working group determines the transfer is in the best interest of the state."*

Given the short timeframe provided by the legislation, and the time it took to secure a vendor through the appropriate procurement process, a working group of state agencies convened by OIT in conjunction with the vendor was able to complete important foundational assessments and preliminary conversations - but further agency working group meetings are still needed.

This report is being submitted to meet the statutory December 1, 2019 deadline and includes important actions to be completed to inform further agency working group conversations. All future actions and recommendations from the working group will be put forward to the IT Steering Committee (an advisory body to provide a forum for executive directors and the OIT leadership to collaborate in the oversight of statewide IT projects and assets) for deliberation and decision.

BACKGROUND

As a result of previous legislation, the State of Colorado has consolidated the Executive Branch agency's IT personnel, some assets, and operations under the management of OIT:

- IT staff from the executive branch agencies were transferred to and are managed by OIT.
- Agency IT assets were moved out of 40 data centers into 3 consolidated State OIT data centers or migrated to cloud services.
- Responsibility for maintaining data center assets, data centers, mainframe, voice and data networks, public safety network, and storage was placed under OIT.
- All of the in-scope agencies have transferred responsibility of maintaining and operating the equipment, but all the funding and decision-making are retained with the agencies, leaving OIT without any corresponding ability to effectively track the assets.

INITIAL ASSESSMENT

To begin this work, OIT hired a vendor to perform an initial assessment of the current state of agencies and assets to inform further conversation.

This assessment found that there are significant security concerns to the state caused by unsupported and unknown equipment. The root cause of these security concerns are agencies not refreshing their IT assets in a timely manner and according to OIT Standards.

- The established standard refresh cycle for IT infrastructure assets is four (4) years. Based on the end-user device data provided, over 38% of asset inventory is due for a refresh. This suggests the established refresh cycle standard is not being followed.
- Over 22% of server instances have reached end of life and are due for a refresh.
- IT assets are overdue for updates, are beyond their useful life, or are no longer supported by the equipment manufacturer. Outdated, vendor-unsupported systems pose significant risk to the state, since manufacturer patches are no longer being released to fix vulnerabilities.
- Current inventory data, based on what is now known by OIT, of end-user devices shows 16 different manufacturers and over 500 models.
- Agencies are currently unable to provide detailed inventory of assets they own, and instead depend on OIT to track and manage these assets. However, a physical inventory is needed to accomplish this fully.

More details on these assessments are attached in Appendix A below.

The vendor facilitated working group meetings with the OIT and agency stakeholders to collect, review, and assess self-reported IT asset data, to identify all known infrastructure located within OIT and agencies, as well as the associated equipment age, refresh date, estimated replacement costs, maintenance costs, and funding source for each. Following the review of asset data and supporting documents, agency interviews were conducted to review any data that needed additional clarification and information from agencies. These interviews were with agency representatives to understand their concerns, needs, and unique agency requirements. The interviews allowed agency representatives a chance to share any preliminary comments or concerns they had about transferring IT assets as well as any unique agency needs.

INITIAL RECOMMENDED ACTIONS

Following the assessment and agency interviews, it was determined that the following additional steps should be accomplished to inform further agency working group conversations on the remaining statutory charge.

1. Complete a full physical inventory of assets, including tagging and documenting the location of all assets in agencies.
2. Set up an Asset Management program and processes, and acquire and implement an asset management tool.
3. Set up a Configuration Management Database.
4. Set up an IT Service Management (ITSM) tool.
5. Establish and maintain workforce training capabilities to educate and enforce the policies for asset management.

OIT's November 1st budget submission for FY 2020-21 includes funding that tangentially helps accomplish some of these initial steps (specifically Actions 2, 3, and 4). However, the working group and IT Steering Committee will continue to explore the need and cost associated with completing a full physical inventory of assets, including tagging and documenting the location of all assets in all agencies, and establishing workforce training capabilities for asset management.

ASSET REFRESH

At this time, the full scope of the need for asset refresh gap is not fully understood. Following the completion of the actions above, a better understanding of refresh needs will be known. OIT will be developing a plan, in collaboration with state agencies and the IT Steering Committee, to identify the immediate and ongoing refresh needs to reach compliance.

DIFFERENT TYPES OF ASSETS

It is important to identify that there are two buckets of IT assets, each necessitating a different level of effort around security and ownership.

- End User Devices - such as desktop and laptop computers, printers, computer peripherals, cell phones, and more.
- Infrastructure - such as the network, servers, data center, storage, applications, managed services, and specialty equipment/devices.

It is the infrastructure that has the highest need for security, due to the shared nature of the assets and ability to protect against, or more widely propagate, security threats.

INTERIM STEPS TO ENSURE SECURITY

The Governor is committed to ensuring a secure State of Colorado. To mitigate potential security risks, OIT and the Governor's Office will ensure agencies are fully aware of OIT standards for asset refresh, as well as full enforcement and agency compliance. To operationalize this, the following steps will be taken:

1. OIT will issue a compliance report on a periodic basis to agency executive directors and the Governor's Office to raise awareness of the non-compliant assets and unsupported software posing a security risk.
2. OIT will perform periodic audits and provide results to agencies to either remediate the non-compliant assets, or certify in writing that they assume the risks.
3. The OIT Security team will work to preemptively remove at-risk assets from the network to ensure they no longer pose a threat .
4. OIT may establish enterprise agreements with technology providers, allowing agencies to buy directly from a vendor, who would be required to configure the asset according to OIT standards and to send OIT the asset refresh data for our records.

NEXT STEPS

Concurrent with implementation of the action items identified above, OIT will convene the working group of state agencies to identify any additional actions needed, as well as further delve into the final question of "*appropriateness of transferring ownership of information technology infrastructure."*

As additional requirements and resource needs are identified, OIT will continue to provide updated information, including plans for implementation and ongoing concerns in future reports and budget requests, as required by statute.

Appendix A -- Additional Assessment Data

A stoplight methodology has been used to help readers interpret the charts provided. In general, the colors have the following meaning:

- Meets or exceeds industry or peer metrics
- Slight variance from industry or peer metrics
- Significant variance from industry or peer metrics
- Not rated due to insufficient data or not in scope

Figure 1: PC Refresh

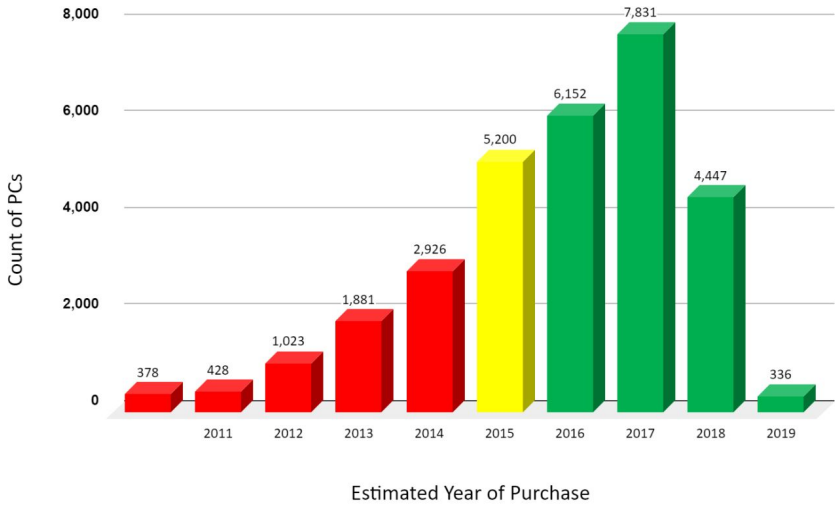

Figure 2: Server Instances (Windows)

Major OS	Major Version	Total Instances	% of Total Instances	Official End of Life
Windows 7	Professional	55	4%	Supported but not recommended for Server OS
Windows XP	Professional	1	0%	Unsupported
W2K	Standard	6	0%	Unsupported
W2K3	Standard	192	14%	Unsupported
W2K8R2	Standard or Enterprise	371	28%	Mainstream 1/15/2015, Extended Support through 1/14/2020
W2K12	Standard or Enterprise	457	34%	Mainstream 1/9/2018, Extended Support through 1/10/2023
W2K16	Standard or Enterprise	267	20%	Mainstream 1/11/2022, Extended Support through 1/12/2027
Totals		1349	100%	

Figure 3: Server Instances (UNIX / Linux Variants)

Major OS	Major Version	Total Instances	% of Total Instances	Official End of Life
CentOS	6	15	2%	General Support End - 05/10/2017 Extended Support End - 11/30/2020
ESXi VMWare	5.1	11	2%	General Support End - 08/24/2016 Extended Support End - 08/24/2018
	5.5	15	2%	General Support End - 08/21/2018 Extended Support End - 08/28/2020
	6.0	5	1%	General Support End - 03/12/2020 Extended Support End - 03/12/2022
HP-UX	11.3	7	1%	General Support End - 12/31/2020
Linux	Unknown	115	16%	Version unknown
Oracle Linux	5	1	0%	General Support End - 2/1/2013 Extended Support End - None
	7	7	1%	General Support End - 7/1/2024 Extended Support End - None
	Unknown	86	12%	Version unknown
Proprietary	Unknown	41	6%	
Redhat Linux	Enterprise 5	5	1%	General Support End - 1/31/2017 Extended Support End - 11/30/2020
	Enterprise 6	48	7%	General Support End - 11/30/2020 Extended Support End - 6/30/2024
	Enterprise 7	123	18%	General Support End -Q4 2020 Extended Support End - None
	Unknown	1	0%	Version unknown
Solaris	9.0	1	0%	General Support End - 1/1/2021 Extended Support End- 1/1/2021
	10.0	18	3%	General Support End - 1/1/2021 Extended Support End- 1/1/2021
	11.0	4	1%	General Support End - 1/1/2021 Extended Support End- 1/1/2021
SUSE Linux	Enterprise 9	5	1%	General Support - 1/31/2019 Extended Support End - None
	Enterprise 10	68	10%	General Support - 1/31/2019 Extended Support End - None
	Enterprise 11	116	17%	General Support - 1/31/2019 Extended Support End - None
	Enterprise 12	2	0%	General Support - 1/31/2019 Extended Support End - None
Ubuntu	16.04 LTS	3	0%	Maintenance updates through Q2 2020
Totals		697	100%	